AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1   1. (Currently amended) A method that facilitates secure electronic

2 commerce, comprising:

3   providing a consumer with a file of security data relating to an account

4 maintained by a financial institution, wherein the file of security data is provided

5 to the consumer on a smart card, and wherein the file of security data includes:

6   a consumer identifier,

7   a private key for encryption and authentication of data,

8   a first public key related to the private key for decryption

9   and authentication of data,

10   an identifier identifying the financial institution,

11   a second public key belonging to the financial institution,

12   the account number that has been encrypted with a key

13   known only to the financial institution creating an encrypted

14   account number,

15   a first certificate signed by a recognized certificate authority

16   that validates the financial institution,

17   a second certificate signed by the financial institution that

18   validates the consumer, and

19   computer algorithms to use the file of security data;

20   creating a financial transaction between the consumer and a merchant,

21 wherein the financial transaction is protected using security data from the file, and

22   wherein the financial transaction is structured to contain an account number in a

23   form that is undecipherable by the merchant, thereby prevent the merchant from

24   knowing the account number for the account, and wherein protecting the financial

25   transaction involves:

26   creating a first hash of the financial transaction, and

27   encrypting the first hash, the second certificate, and the

28   encrypted account number using the second public key creating a

29   secure envelope of transaction data, wherein the first hash is

30   created at a secure site available only to the consumer;

31   validating by the merchant that the financial institution identified by the

32   financial transaction is acceptable using security data from the file;

33   wherein validating by the merchant involves:

34   receiving at the merchant the first certificate; and

35   validating that the first certificate was signed by the recognized certificate

36   authority;

37   requesting by the merchant that the financial institution authorize the

38   financial transaction;

39   receiving by the merchant an authorization from the financial institution to

40   complete the financial transaction;

41   completing the financial transaction between the consumer and the

42   merchant; and

43   notifying the financial institution that the financial transaction is complete.

1   2-4 (Canceled).

1   5. (Currently amended) The method of claim 4 claim 1, wherein requesting

2   by the merchant that the financial institution authorize the financial transaction

3   involves:

4   creating a second hash of the financial transaction by the merchant;

5   sending the secure envelope and the second hash to the financial

6 institution;

7   decrypting at the financial institution the secure envelope using the private

8 key of the financial institution;

9   comparing the first hash with the second hash; and

10   if the first hash is identical to the second hash,

11   decrypting the encrypted account number to recover the

12   account number for the account belonging to the consumer,

13   verifying that the financial transaction is valid for the

14   account, and

15   if valid, authorizing the financial transaction.

1   6. (Original) The method of claim 5, wherein verifying that the financial

2 transaction is valid for the account includes:

3   verifying that the second certificate was signed by the financial institution;

4   determining that the account is valid; and

5   ensuring that a transaction amount is not greater than an authorized

6 transaction amount.

1   7. (Currently amended) The method of ~~claim 4~~ claim 1, wherein the secure

2 site available only to the consumer is within the smart card.

1   8 (Canceled)

1   9. (Currently amended) A computer-readable storage medium storing

2 instructions that when executed by a computer cause the computer to perform a

3 method that facilitates secure electronic commerce, comprising:

4   providing a consumer with a file of security data relating to an account

5   maintained by a financial institution, wherein the file of security data is provided

6   to the consumer on a smart card , and wherein the file of security data includes:

7   a consumer identifier,

8   a private key for encryption and authentication of data,

9   a first public key related to the private key for decryption

10   and authentication of data,

11   an identifier identifying the financial institution,

12   a second public key belonging to the financial institution,

13   the account number that has been encrypted with a key

14   known only to the financial institution creating an encrypted

15   account number,

16   a first certificate signed by a recognized certificate authority

17   that validates the financial institution,

18   a second certificate signed by the financial institution that

19   validates the consumer,

20   computer algorithms to use the file of security data;

21   creating a financial transaction between the consumer and a merchant,

22   wherein the financial transaction is protected using security data from the file, and

23   wherein the financial transaction is structured to contain an account number in a

24   form that is undecipherable by the merchant, thereby prevent the merchant from

25   knowing the account number for the account, and wherein protecting the financial

26   transaction involves:

27   creating a first hash of the financial transaction, and

28   encrypting the first hash, the second certificate, and the

29   encrypted account number using the second public key creating a

30   secure envelope of transaction data, wherein the first hash is

31   created at a secure site available only to the consumer;

32   validating by the merchant that the financial institution identified by the

33   financial transaction is acceptable using security data from the file;

34   wherein validating by the merchant involves:

35   receiving at the merchant the first certificate; and

36   validating that the first certificate was signed by the recognized certificate

37   authority;

38   requesting by the merchant that the financial institution authorize the

39   financial transaction;

40   receiving by the merchant an authorization from the financial institution to

41   complete the financial transaction;

42   completing the financial transaction between the consumer and the

43   merchant; and

44   notifying the financial institution that the financial transaction is complete.

1   10-12 (Canceled).

1   13. (Currently amended) The computer-readable storage medium of claim

2   12 claim 9, wherein requesting by the merchant that the financial institution

3   authorize the financial transaction involves:

4   creating a second hash of the financial transaction by the merchant;

5   sending the secure envelope and the second hash to the financial

6   institution;

7   decrypting at the financial institution the secure envelope using the private

8   key of the financial institution;

9   comparing the first hash with the second hash; and

10   if the first hash is identical to the second hash,

11   decrypting the encrypted account number to recover the

12   account number for the account belonging to the consumer,

6

13   verifying that the financial transaction is valid for the

14   account, and

15   if valid, authorizing the financial transaction.

1   14. (Original) The computer-readable storage medium of claim 13,

2 wherein verifying that the financial transaction is valid for the account includes:

3   verifying that the second certificate was signed by the financial institution;

4   determining that the account is valid; and

5   ensuring that a transaction amount is not greater than an authorized

6 transaction amount.

1   15. (Currently amended) The computer-readable storage medium of ~~claim~~

2 ~~12~~ claim 9, wherein the secure site available only to the consumer is within the

3 smart card.

1   16 (Canceled)

1   17. (Currently amended) An apparatus that facilitates secure electronic

2 commerce, comprising:

3   a providing mechanism configured to provide a consumer with a file of

4 security data relating to an account maintained by a financial institution, wherein

5 the file of security data is provided to the consumer on a smart card , and wherein

6 the file of security data includes:

7   a consumer identifier,

8   a private key for encryption and authentication of data,

9   a first public key related to the private key for decryption

10   and authentication of data,

11   an identifier identifying the financial institution,

7

12	a second public key belonging to the financial institution,
13	the account number that has been encrypted with a key
14	known only to the financial institution creating an encrypted
15	account number,
16	a first certificate signed by a recognized certificate authority
17	that validates the financial institution,
18	a second certificate signed by the financial institution that
19	validates the consumer, and
20	computer algorithms to use the file of security data;
21	a first creating mechanism configured to create a financial transaction
22	between the consumer and a merchant, wherein the financial transaction is
23	protected using security data from the file, and wherein the financial transaction is
24	structured to contain an account number in a form that is undecipherable by the
25	merchant, thereby prevent the merchant from knowing the account number for the
26	account;
27	a second creating mechanism that is configured to create a first hash of the
28	financial transaction; and
29	an encrypting mechanism that is configured to encrypt the first hash, the
30	second certificate, and the encrypted account number using the second public key
31	creating a secure envelope of transaction data, wherein the first hash is created at a
32	secure site available only to the consumer;
33	a first validating mechanism that is configured to validate that the financial
34	institution identified by the financial transaction is acceptable using security data
35	from the file;
36	a second receiving mechanism at the merchant that is configured to receive
37	the first certificate; and
38	a second validating mechanism that is configured to validate that the first
39	certificate was signed by the recognized certificate authority;

8

40 a requesting mechanism that is configured to request that the financial

41 institution authorize the financial transaction;

42 a first receiving mechanism that is configured to receive an authorization

43 from the financial institution to complete the financial transaction;

44 a completing mechanism that is configured to complete the financial

45 transaction between the consumer and the merchant; and

46 a notifying mechanism that is configured to notify the financial institution

47 that the financial transaction is complete.

1 18-20 (Canceled).

1 21. (Currently amended) The apparatus of claim 20 claim 17, further

2 comprising:

3 a creating mechanism that is configured to create a second hash of the

4 financial transaction by the merchant;

5 a sending mechanism that is configured to send the secure envelope and

6 the second hash to the financial institution;

7 a decrypting mechanism that is configured to decrypt the secure envelope

8 using the private key of the financial institution;

9 a comparing mechanism that is configured to compare the first hash with

10 the second hash;

11 wherein the decrypting mechanism is further configured to decrypt the

12 encrypted account number to recover the account number for the account

13 belonging to the consumer;

14 a first verifying mechanism that is configured to verify that the financial

15 transaction is valid for the account; and

16 an authorizing mechanism that is configured to authorize the financial

17 transaction.

9

1   22. (Original) The apparatus of claim 21, further comprising:

2   a second verifying mechanism that is configured to verify that the second

3 certificate was signed by the financial institution;

4   a determining mechanism that is configured to determine that the account

5 is valid; and

6   an ensuring mechanism that is configured to ensure that a transaction

7 amount is not greater than an authorized transaction amount.

1   23. (Currently amended) The apparatus of ~~claim 20~~ claim 17, wherein the

2 secure site available only to the consumer is within the smart card.

1   24 (Canceled)